

# Classical light steering leading to quantum-like security

Tanumoy Pramanik<sup>1,\*</sup> and A. S. Majumdar<sup>1,†</sup>

<sup>1</sup>*S. N. Bose National Centre for Basic Sciences,  
Block JD, Sector III, Salt Lake, Kolkata 700098, India*

(Dated: June 28, 2016)

We show how single system steering can be exhibited by classical light, a feature originating from superposition in classical optics that also enables entanglement and Bell-violation by classical light beams. Single system steering is the temporal analogue of Einstein-Podolsky-Rosen (EPR) steering in the quantum domain, enabling control of the state of a remote system, and can hence be connected to the security of secret key generation between two remote parties. We derive the steering criterion for a single mode coherent state when displaced parity measurements are performed at two different times. The security bound of the Bennett-Brassard 1984 (BB84) protocol under the gaussian cloning attack is calculated to yield an, in principle, ideal and quantum-like key rate using a fine-grained uncertainty relation corresponding to the classical phase space.

PACS numbers: 03.67.-a, 03.67.Mn

In the quantum world the superposition principle plays a fundamental role in nearly all phenomena, without which it would be impossible for entanglement to exist and be used as resource for performing quantum information processing tasks. Among the many examples of quantum information processing, quantum key distribution (QKD) is one of the most widely studied [1–5], in view of its importance in the practical demonstration of the quantum advantage over corresponding classical information processing protocols. The security of QKD protocols is guaranteed, in principle, by quantum uncertainty [2], and is further linked in entanglement based protocols to quantum nonlocality [3, 4] and quantum steering [5]. The first QKD protocol to be proposed, *viz.* the BB84 protocol is based on the superposition principle with its security ensured by the uncertainty relations.

The relevance of superposition in physics, is however, not exclusive to the quantum domain. The importance of superposition in classical wave theory was manifested through interference and diffraction phenomena long before the advent of quantum theory. In modern times classical optical coherence is utilized in wide ranging applications such as holographic interferometry [6] and magneto-optical Kerr effect [7] in the study of structure of materials, to interferometric telescopes and Hanbury Brown-Twiss effect [8] in astronomy. Classical light beams with non-trivial topological structure have been discovered [9] with applications in optical tweezers [10], and are regarded to be potentially useful for information processing due to their ability to carry large amounts of information [11].

The key role of superposition common to both quantum mechanics and classical optics has lead to the formulation of uncertainty relations in the latter analogously to the well-known uncertainty principle of the

former [12, 13]. In wave optics the wavelength of light  $\lambda = \lambda/2\pi = c/\omega$  plays a role analogous to the Planck's constant  $\hbar$  in quantum mechanics. The finite and non-vanishing wavelength  $\lambda$  leads to the lack of precision in simultaneous measurement of two incompatible observables. In other words, relationships analogous to the Heisenberg uncertainty relation, such as

$$(\Delta\hat{x}^2)(\Delta\hat{p}^2) \geq \frac{\lambda^2}{4} \quad (1)$$

are obtained between observables corresponding to the position space and the wave vector space due to the finite and non-vanishing wave vector  $k \sim 1/\lambda$  involved in fourier transformation connecting these two domains. The above analogy results in mathematical isomorphism for correlations between physical degrees of freedom in classical optics in relation with quantum entanglement in two-qubit systems, thus inspiring the formulation of the theory of classical entanglement [14] and violation of Bell inequalities [15] in classical electromagnetism [16, 17]. In particular, Schmidt decomposition pertaining to superposition of classical electromagnetic fields [18] has been exploited to derive Bell-like inequalities [17] for classical vortex beams [19]. Such Bell violation in the domain of classical continuous variable phase space has been experimentally verified too [20].

Other than entanglement and Bell nonlocality, another form of correlation in quantum mechanics is exemplified by EPR steering [21]. Steering entails the ability to control the state of a remote system through local measurements. Formulation of correlations in terms of their applicability in information theoretic tasks involving two distant parties enables understanding of quantum steering as an intermediate correlation between entanglement and Bell nonlocality [22]. Besides the above types of spatial correlations, the quantum framework accommodates certain temporal correlations, such as those quantified by the Leggett-Garg inequality [23], as well as temporal steering or single system steering [24]. Inspired by the above analogy in features of classical optics and quan-

\*Electronic address: tanu.pram99@bose.res.in

†Electronic address: archan@bose.res.in

tum mechanics, such as superposition, entanglement and Bell violation, we are thus motivated to enquire as to what task analogous to quantum steering may be implementable in classical optics.

In the present work we develop a protocol for single system steering in classical optics. Quantum steering of single systems has been formulated recently [24], and shown to have applications in the security of the BB84 key distribution protocol, as well as in quantifying non-Markovianity [25]. All steerability conditions arise from uncertainty relations which form the underlying basis of security in key distribution protocols. EPR steering has been linked directly to the key rate of one-sided device independent key distribution [5], and similarly, single system steering to the BB84 key distribution [24]. Optimal steering relations have been derived [26] using the fine-grained uncertainty relation that connects uncertainty with nonlocality in quantum mechanics [27]. A continuous variable fine-grained steering inequality has also been derived which leads to an, in principle, ideal key rate in one-sided device independent key distribution [28]. Here, in order to derive an optimal steering inequality in classical electromagnetism, we first formulate a fine-grained uncertainty relation in classical phase space. Our fine-grained steering condition thus forms the basis for the single systems steering protocol in classical optics, and is finally used to obtain an, in principle, ideal key rate for the BB84 protocol using a single mode coherent state.

We begin by discussing briefly the key features of uncertainty in the phase space of classical optics [12, 13, 17]. In paraxial optics the propagation of a light beam  $E(\vec{r}; t) = \varepsilon(\vec{r}) \left( \frac{i\omega z}{c} - i\omega t \right)$  in free space is described by  $i\frac{\partial \varepsilon}{\partial z} = -\frac{\lambda}{2} \nabla_k^2 \varepsilon$ , (with  $\lambda = \lambda/2\pi = c/\omega$  and  $k = x, y$ ), which is, for  $t \rightarrow z$ ,  $\psi \rightarrow \varepsilon$ ,  $\hbar \rightarrow \lambda$ , exactly the Schrodinger equation for a free particle in two dimensions. Here  $\lambda \rightarrow 0$  leads to the limit of geometrical optics in a similar way as  $\hbar \rightarrow 0$  yields the classical limit of quantum mechanics. Therefore, any optical beam in two dimensions can be written as superposition of the solutions of the above equation. For example, eigenfunctions of the two dimensional harmonic oscillator can be expressed as Laguerre-Gaussian beams constructed from the superposition of Hermite-Gaussian functions [19]. Exploiting this feature, classical entanglement and Bell violation has been demonstrated for Laguerre-Gaussian beams [17]. The quadrature amplitudes corresponding to the field  $E_{\alpha_j} \propto \hat{a} \exp^{-i\omega_{\alpha_j} t} + \hat{a}^\dagger \exp^{i\omega_{\alpha_j} t}$  (with the two modes denoted by  $\alpha_j$   $j = 1, 2$ ) may be written as  $\hat{X}_i^{\theta_j} = \frac{\hat{a}_i \exp(-i\theta_i) + \hat{a}_i^\dagger \exp(i\theta_i)}{\sqrt{2}}$ , where  $\hat{a}_i = \frac{X_i + iP_i}{\sqrt{2}}$ , in terms of the dimensionless variables  $X_i$  and  $P_i$  defined as  $X_i = \frac{\sqrt{2}x_i}{\sigma}$  and  $P_i = \frac{\sigma p_i}{\sqrt{2}\lambda}$ , with  $\sigma$  being any suitable parameter of length dimensions, for instance, the beam waist in the case of Laguerre-Gaussian beams [17], or the initial position space width of Gaussian beams. Therefore, the commutation relations  $[\hat{x}_i, \hat{p}_j] = i\lambda\delta_{ij}$  become  $[\hat{X}_i, \hat{P}_j] = i\delta_{ij}$ , with  $\hat{P}_i = -i\frac{\partial}{\partial X_i}$ , leading to

$[\hat{a}_i, \hat{a}_j] = \delta_{ij}$ . Thus, the Heisenberg type uncertainty relation for the dimensionless phase space variables  $X$  and  $P_X$ , is obtained from  $(\Delta X^2) (\Delta P_X^2) \geq \langle [X, P_X] \rangle^2$ , and is given by

$$(\Delta X^2) (\Delta P_X^2) \geq \frac{1}{4}. \quad (2)$$

Limitations of the Heisenberg uncertainty relation in quantum mechanics [29] were noted soon after its formulation by Schrodinger and Robertson [30] who presented an improved version for any two arbitrary observables. Subsequently, a number of works were performed to alleviate inadequacies such as the state dependence of the lower bound of uncertainty, as well as to develop the uncertainty relation for information theoretic purposes (see the reviews [31, 32]). An entropic uncertainty relation (where uncertainty is measured by Shannon entropy) was derived in wave mechanics [33] with the help of the  $(p, q)$ - norm of the Fourier transformation. It is now accepted that to characterize different tasks in quantum information theory, entropy as a measure of uncertainty is more useful than standard deviation [34]. For example, entropic uncertainty relations show quantum steering by certain continuous variable non-Gaussian states [35], which is failed to be revealed by the Heisenberg uncertainty relation. The entropic uncertainty relation corresponding to our classical wave mechanical phase space directly follows from the work of Bialynicki-Birula and Mycielski [33], and is given by

$$\mathcal{H}(X) + \mathcal{H}(P_X) \geq \ln(\pi e), \quad (3)$$

where  $\mathcal{H}(X) = \int dX |\Psi(X)|^2 \ln |\Psi(X)|^2$  and  $\mathcal{H}(P_X) = \int dk_X |\Psi(k_X)|^2 \ln |\Psi(k_X)|^2$ , with  $\Psi(X)$  and  $\Psi(k_X)$  the position space and wave vector space wave functions, respectively. The entropic uncertainty relation (3) implies the Heisenberg uncertainty relation (2) [33], since the two uncertainty relations (2) and (3) are connected by the inequality  $-\mathcal{H}(\alpha) \leq \frac{1}{2} \ln(2\pi e \Delta \alpha^2)$ , where  $\alpha \in \{X, P_X\}$ .

It has been recently realized that it is possible to construct several quantum games where coarse grained uncertainty relations, such as the Heisenberg and entropic uncertainty relations (where uncertainty is measured in a coarse grained way by taking the average of uncertainty over all possible measurement outcomes) fail to give optimal payoff [27, 36]. Fine-grained forms of uncertainty relations are able to handle such situations better by quantifying uncertainty directly in terms of probabilities of getting particular measurement outcomes and their combinations. Fine-graining reveals the connection of uncertainty with nonlocality of the underlying physical theory for bipartite and tripartite qubit quantum games [27, 37]. Fine-grained uncertainty relations have been further used to derive optimal steerability conditions for both discrete [26] and continuous [28] variable systems. The fine-grained uncertainty relation relevant to the phase space considered here may be obtained with the help of displaced parity measurement of  $\Pi(\beta) = \Pi^+(\beta) - \Pi^-(\beta)$ , where  $\Pi^+(\beta) = \mathcal{D}(\beta) \sum_{n=0}^{\infty} |2n\rangle \langle 2n| \mathcal{D}^\dagger(\beta)$ , and

$\Pi^-(\beta) = \mathcal{D}(\beta) \sum_{n=0}^{\infty} |2n+1\rangle\langle 2n+1| \mathcal{D}^\dagger(\beta)$  correspond to even and odd parity operators, respectively, with  $D(\beta) = \exp[\beta b^\dagger - \beta^* b]$  being the displacement operator.  $\Pi(\beta)$  and  $\Pi(-\beta)$  are associated with uncertainty relations [28]. The displacements “ $+\beta$ ” and “ $-\beta$ ” are chosen with the probabilities  $P_\beta$  and  $P_{-\beta}$ , respectively, with  $P_\beta + P_{-\beta} = 1$ . Labelling the probabilities for getting odd (even) parity measurement outcomes by  $b = 0$  ( $b = 1$ ), the probability distribution  $[P_\beta P(b_\beta) + P_{-\beta} P(b_{-\beta})]$  is bounded by [28]

$$\frac{1}{4} \leq [P_\beta P(b_\beta = 0) + P_{-\beta} P(b_{-\beta} = 0)] \leq \frac{3}{4}, \quad (4)$$

In order to see the connection [32] between the entropic and fine-grained forms of uncertainty relations, consider the Rényi entropy of order  $\eta$  given by  $\mathcal{H}_\eta = \frac{1}{1-\eta} \log(\sum_{b=1}^n p^\eta(b))$ . Shannon entropy is the Rényi entropy with order  $\eta \rightarrow 1$ , while Min-entropy is the Rényi entropy with order  $\eta \rightarrow \infty$  defined by  $H_\infty = \min_b [-\log P(b)] = -\log \max_b P(b)$ . Now, setting  $P_\beta = 1/2 = P_{-\beta}$  for simplicity, and using the concavity of the log function, it follows that  $\frac{1}{2} \mathcal{H}_\infty(\beta) + \frac{1}{2} \mathcal{H}_\infty(-\beta) \geq -\log \max [\frac{1}{2} P(b_\beta) + \frac{1}{2} P(b_{-\beta})]$ . Next, using the second inequality in Eq.(4), one gets  $\mathcal{H}_\infty(\beta) + \mathcal{H}_\infty(-\beta) \geq -2 \log \frac{3}{4}$ , which is of the form similar to the entropic uncertainty relation given by Eq.(3).

Using the above fine-grained uncertainty relation (4), we are now equipped to present our protocol for steering in classical wave optics. In the usual EPR steering scenario [22, 34, 38], Alice prepares systems  $A$  and  $B$  in the bipartite quantum state  $\rho_{AB}$  and sends the system  $B$  to Bob. Bob accepts that the shared state  $\rho_{AB}$  is steerable, only when Alice can control the state of the system  $B$ , which is demonstrated by the violation of a suitable steering inequality based upon the corresponding uncertainty relation. However, in the temporal steering scenario [24, 25], Alice prepares a single quantum systems  $A$  in a well known state (by measuring the system in certain basis)  $\sigma_A$  at time  $t_1$  and sends the system to Bob who checks her control over the state of that system at a later time  $t_2$ . If no noise effects such as environmental decoherence, or eavesdropping occurs in the elapsed interval  $(t_2 - t_1)$ , Alice has complete information about the state of  $A$ , and she can thus project the state in any basis by communicating a suitable unitary rotation to Bob. Temporal steering conditions are mathematically similar to the EPR steering inequalities.

The temporal steering criterion relevant to our present work may be obtained by considering the following game. Alice first prepares a large number of identical systems labeled by  $A$  in single mode coherent state given by [44]

$$|\alpha\rangle_A = \exp\left[-\frac{|\alpha|^2}{2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle_A\right], \quad (5)$$

Next, at time  $t_1$ , she randomly applies either the displacement operator  $\mathcal{D}(\beta)$  or  $\mathcal{D}(-\beta)$ , where, for simplicity, we consider  $\beta$  to be real. Therefore, the system  $A$  is

prepared in the states  $|\alpha + \beta\rangle_A$  and  $|\alpha - \beta\rangle_A$  with the probabilities  $P_{\alpha+\beta}$  and  $P_{\alpha-\beta}$ , respectively. The probability of getting parity measurement outcome  $a$  ( $a = 0$  for even parity and  $a = 1$  for odd parity) for the state chosen from the set  $\{|\alpha + \beta\rangle, |\alpha - \beta\rangle\}$  is bounded by the uncertainty relation (4)

$$\frac{1}{4} \leq [P_{\alpha+\beta} P(a_{\alpha+\beta}) + P_{\alpha-\beta} P(a_{\alpha-\beta})] \leq \frac{3}{4}, \quad (6)$$

where  $P(a_{\alpha\pm\beta})$  is the probability of obtaining the outcome  $a$  for the state  $|\alpha\pm\beta\rangle$ , and the values  $\{\alpha \rightarrow 0 \text{ \& } \beta \rightarrow 0\}$  are excluded [28]. After this Alice sends the system  $A$  to Bob who does not have any prior knowledge of the state of the system. Alice then communicates to Bob over a public channel informing him to apply the displacement operator  $\mathcal{D}(\gamma_1)$  when the prepared state is  $|\alpha + \beta\rangle$ , and  $\mathcal{D}(\gamma_2)$  for the prepared state  $|\alpha - \beta\rangle$ . To check Alice's steerability, Bob measures at time  $t_2$  the parity of the displaced set of states  $\{\mathcal{D}(\gamma_1)|\alpha + \beta\rangle, \mathcal{D}(\gamma_2)|\alpha - \beta\rangle\}$ .

For noiseless channels shared between Alice and Bob, the state sent by Alice is the same as the state received by Bob. Therefore, Alice has full control over Bob's system. In practice, the channels are not ideal due to environmental interaction or interruption by a third party. Noise introduces unexpected uncertainty in the conditional probability of Bob's measurement outcome given Alice's preparation. The (non-)steerability condition may be derived by assuming that noise makes the states  $|\alpha \pm \beta\rangle$  end up in an unknown state  $\sigma_\lambda$  with the conditional probability  $P(\lambda|\alpha \pm \beta)$ . Bob thus receives the system  $A$  in the state  $\sigma_B(\alpha \pm \beta) = \sum_{k=0}^1 \sum_\lambda P(\alpha + (-1)^k \beta) P(\lambda|\alpha + (-1)^k \beta) \sigma_\lambda = \sum_\lambda P(\lambda) \sigma_\lambda$ , when the prepared state is  $|\alpha \pm \beta\rangle$ . It is clear that Bob's state  $\sigma_B$  is independent of Alice's preparation procedure. Hence, Alice does not have any control over the state  $\sigma_B$ , i.e., the state is unsteerable. The sum of probabilities obtained using the state  $\sigma_B(\alpha \pm \beta)$  and also the state  $\mathcal{D}(\gamma_1)\sigma_B(\alpha \pm \beta)\mathcal{D}^\dagger(\gamma_1)$  satisfy the inequality (6).

On the other hand, if Alice has control over Bob's system, Bob can reduce his uncertainty about measurement outcomes when Alice sends the information about the displacement operator. The sum of the conditional probabilities of getting the outcome  $b$  for the parity measurement after applying the displacement operator  $\mathcal{D}(\gamma_1)$  by Bob for the prepared state  $|\alpha + \beta\rangle_A$  and for the case when Bob applies the displacement operator  $\mathcal{D}(\gamma_2)$  for the prepared state  $|\alpha - \beta\rangle_A$ , i.e.,  $(P_{\alpha+\beta} P(b_{\gamma_1}|\alpha + \beta) + P_{\alpha-\beta} P(b_{\gamma_2}|\alpha - \beta))$  will lie outside of the region  $[1/4, 3/4]$  in this case. Therefore, temporal steerability occurs when either of the two inequalities

$$\frac{1}{4} \leq [P_{\alpha+\beta} P(b_{\gamma_1}|\alpha + \beta) + P_{\alpha-\beta} P(b_{\gamma_2}|\alpha - \beta)] \leq \frac{3}{4}, \quad (7)$$

is violated. For example, with the choice of displacements  $\gamma_1 = -\alpha - \beta$  and  $\gamma_2 = -\alpha + \beta$ , the sum of probabilities is plotted versus  $\beta$  and  $P_{\alpha+\beta}$  in the Figure 1, showing that the state (5) is steerable in

the ranges  $0 < p < \frac{\sqrt{2}\sqrt{2e^{-8\beta^2}-3e^{-4\beta^2}+1}+2e^{-4\beta^2}-2}{4(e^{-4\beta^2}-1)}$  and  $\frac{-\sqrt{2}\sqrt{2e^{-8\beta^2}-3e^{-4\beta^2}+1}+2e^{-4\beta^2}-2}{4(e^{-4\beta^2}-1)} < p < 1$ . Specifically, if

Alice has full control over Bob's system, the probability of getting even parity is unity for  $\gamma_1 = -\alpha - \beta$  and  $\gamma_2 = -\alpha + \beta$ , and similarly, the probability of getting odd parity is unity for the choice  $\gamma_1 = 1 - \alpha - \beta$  and  $\gamma_2 = 1 - \alpha + \beta$ . Note that the above steerability condition is obtained in the context of classical optics, and is based on the fine-grained uncertainty relation (4) for classical phase space variables. One may obtain similar steerability conditions in classical optics based on other forms of uncertainty relations such as those given by Eqs.(2) and (3). Here we employ the fine-grained form of uncertainty since it provides an optimal steerability condition for continuous variables [28].

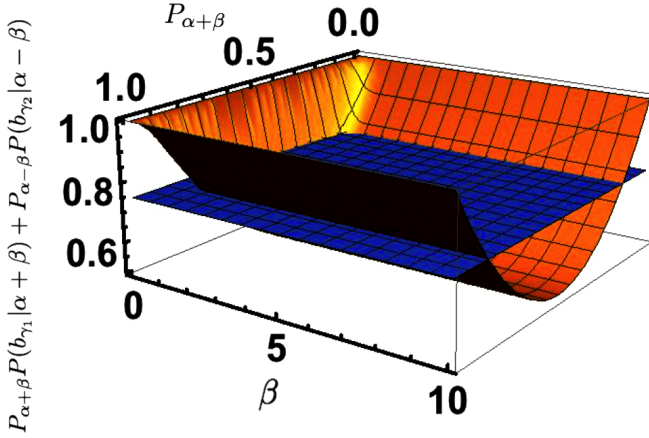


FIG. 1: Steerability of the state (5) for the choice  $\gamma_1 = -\alpha - \beta$  and  $\gamma_2 = -\alpha + \beta$ . The curved and plane surfaces represent the sum of probabilities and the upper bound, respectively, in Eq.(7).

Temporal steering is connected to the security of the BB84 protocol [2] of key generation, as was shown for the case of discrete variables [24] in quantum mechanics. Here we discuss the security of a key generation scenario in classical optics similar to the BB84 protocol using continuous variables. Here, Alice prepares an ensemble of systems  $A$  either in the coherent state  $|\alpha + \beta\rangle$  or in  $|\alpha - \beta\rangle$ . When Alice sends the systems  $A$  to Bob, an eavesdropper, Eve can clone the system to gain information about it. Perfect cloning is disallowed in quantum mechanics as it would enable determination of two incompatible observables through an arbitrarily large number of cloned copies. Perfect cloning is impossible in the phase space of classical optics in order to preserve the uncertainty relation (2), analogously to the case of quantum mechanics where perfect cloning is forbidden in order to preserve the quantum uncertainty principle [39]. In continuous variable systems the optimal strategy of cloning is achieved using the Gaussian cloning machine [40] by which coherent states are cloned with the optimal fidelity  $2/3$ . The operation of the Gaussian cloning on the state  $|\alpha \pm \beta\rangle_A$

leads to

$$|\alpha \pm \beta\rangle_A |0\rangle_E \rightarrow |(\alpha \pm \beta) \cos |\eta|\rangle_A |(\alpha \pm \beta) \frac{\eta}{|\eta|} \sin |\eta|\rangle_E, \quad (8)$$

where  $|0\rangle_E$  the initial state of Eve's system and  $\eta$  is the cloning parameter. Considering application of the displacement operators  $\gamma_1 = -\alpha - \beta$  or  $\gamma_2 = -\alpha + \beta$ , due to Eve's interception at the time of its transit, the final state of the system  $A$  becomes  $|(\alpha + \beta) (\cos |\eta| - 1)\rangle_A$  or  $|(\alpha - \beta) (\cos |\eta| - 1)\rangle_A$ . When Alice tries to create an even (0) parity state on Bob's side, she informs him of the choice of displacement  $\gamma_1 = -\alpha - \beta$  for her prepared state  $\alpha + \beta\rangle_A$ , or  $\gamma_2 = -\alpha + \beta$  for her prepared state  $\alpha - \beta\rangle_A$ . However, error occurs due to eavesdropping, and hence, the probability of getting odd parity (1) by Bob becomes

$$\begin{aligned} P_{01}(\alpha \pm \beta) &= \sum_{m=0}^{\infty} |\langle 2m+1 | (\alpha \pm \beta) (\cos |\eta| - 1) \rangle_A|^2 \\ &= \sinh(|\delta|^2) \exp\left(-\frac{|\delta|^2}{2}\right), \end{aligned} \quad (9)$$

where  $\delta = (\alpha \pm \beta) (\cos |\eta| - 1)$ , and for simplicity we take  $P_{\alpha+\beta} = 1/2 = P_{\alpha-\beta}$ . As Alice randomly prepares the system  $A$  either in the state  $|\alpha + \beta\rangle_A$  or in the state  $|\alpha - \beta\rangle$ . The average error is given by  $P_{01} = \frac{1}{2} P_{01}(\alpha + \beta) + \frac{1}{2} P_{01}(\alpha - \beta)$ . The correlation between Alice and Bob is quantified by mutual information,  $\mathcal{I}(A : B)$  which is defined by  $\mathcal{I}(A : B) = \mathcal{H}(A) - \mathcal{H}(B|A)$ , where  $\mathcal{H}$  is Shannon entropy. As Alice randomly prepares system  $A$  in the state  $|\alpha \pm \beta\rangle_A$ ,  $\mathcal{H}(A) = 1$ , and  $\mathcal{H}(B|A)$  is given by  $\mathcal{H}(P_{01})$ . The error in correlation between Alice and Bob is thus given by  $\mathcal{I}^E(A : B) = 1 - \mathcal{H}(P_{01})$ .

Similarly, the error corresponding to case when the eavesdropper Eve obtains odd parity while Alice tries to control Bob's state in even parity becomes

$$\begin{aligned} Q_{01}(\alpha \pm \beta) &= \sum_{m=0}^{\infty} |\langle 2m+1 | (\alpha \pm \beta) \left(\frac{\eta}{|\eta|} \sin |\eta| - 1\right) \rangle_A|^2 \\ &= \sinh(|\delta'|^2) \exp\left(-\frac{|\delta'|^2}{2}\right), \end{aligned} \quad (10)$$

where  $\delta' = (\alpha \pm \beta) \left(\frac{\eta}{|\eta|} \sin |\eta| - 1\right)$ . Here, the average error is given by  $Q_{01} = \frac{1}{2} Q_{01}(\alpha + \beta) + \frac{1}{2} Q_{01}(\alpha - \beta)$ , where we consider  $P_{\alpha+\beta} = P_{\alpha-\beta} = \frac{1}{2}$  because randomness gives maximum error. In this case, the error mutual information is given by  $\mathcal{I}^E(A : E) = 1 - \mathcal{H}(Q_{01})$ . Thus, the bound on the error rate is given by [41]  $r_e = \mathcal{I}(A : B) - \max_{Eve} \mathcal{I}^E(A : E)$ , where maximization is taken over all possible Eve's strategies. Here, the maximum occurs for  $\eta = \pi/4$  and corresponding error rate becomes 0. Such a result is analogous to the key rate obtained to be  $r = 1$  for quantum continuous variable systems derived using the fine-grained uncertainty relation [28].

To summarize, in the present work we have derived a temporal steering criterion in classical optics. Recently,

quantum steering [21, 22] has been recast as the control of a single quantum system at different times, with the formulation of a temporal steering scenario for discrete variable quantum systems [24, 25]. Here, by developing further the analogy between quantum mechanics and classical wave optics emanating from the key feature of superposition in both the theories [12–14, 16, 17], we first formulate a fine-grained uncertainty relation in the realm of the latter. An optimal [26, 28] steering inequality thus follows using displaced parity operations on a single mode coherent state. Further, exploiting the connection between temporal steering and the secret key rate of the BB84 protocol, here we derive an analogous, and in principle, ideal key rate in classical optics. Note that though

continuous variable quantum key generation using coherent states has been proposed earlier [42], the security therein is based on the quantum uncertainty principle. On the other hand, the security of key generation discussed here is based fundamentally upon the uncertainty relation (1) in classical wave optics. Besides exploring possible practical ramifications of this difference, it may also be interesting to perform further investigations on the ontological nature of a classical wave theory that permits steering and disallows perfect cloning, vis-a-vis its quantum counterpart [43].

*Acknowledgements:* The authors acknowledge support from the project SR/S2/LOP-08/2013 of DST, India.

- 
- [1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
  - [2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computer, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175-179.
  - [3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
  - [4] D. Mayers, Quant. Inf. Comp. **4**, 273 (2004); A. Acín, N. Gisin, and L.I. Masanes, Phys. Rev. Lett. **97**, 120405 (2006); A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007); S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009); U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
  - [5] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011); C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).
  - [6] C. M. Vert, *Holographic Interferometry*, (J. Wiley & Sons, N.Y., 1979)
  - [7] D. A. Allwood, G. Xiong, M. D. Cooke, R. P. Cowburn, J. Phys. D: Applied Phys. **36**, 2175 (2003).
  - [8] R. Hanbury Brown, *The intensity interferometer; its application to astronomy*, (Taylor & Francis, 1974).
  - [9] J. F. Nye and M. V. Berry, Proc. R. Soc. London Ser. A **165**, 336 (1974).
  - [10] D. G. Grier, Nature **424**, 810 (2003).
  - [11] G. Molina-Terriza, J. P. Torres, L. Torner, Nature Phys. **3**, 305 (2007); R. Fickler et al., Science **338**, 640 (2012).
  - [12] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics* (Wiley, New Jersey, 2007), p 48.
  - [13] M. Mansuripur, *Classical optics and its applications*, (CUP Cambridge, 2009), p 258.
  - [14] R. J. C. Spreeuw, Found. Phys. **28**, 361 (1998); A. Aiello and J. P. Woerdman, Phys. Rev. Lett. **94**, 090406 (2005); X-F. Qian and J. H. Eberly, Opt. Lett. **36**, 4110 (2011); B. N. Simon et al, Phys. Rev. Lett. **104**, 023901 (2010); P. Ghose, A. Mukherjee, Rev. Theor. Science **2**, 1 (2014); A. K. Rajagopal, P. Ghose, arXiv: 1409.5874.
  - [15] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964); J. F. Clauser, M. A. Horne, A. Shimony et al., Phys. Rev. Lett. **23**, 880 (1969).
  - [16] K. H. Kagalwala et al., Nature Photonics **7**, 72 (2013).
  - [17] P. Chowdhury, A. S. Majumdar, G. S. Agarwal, Phys. Rev. A **88**, 013830 (2013).
  - [18] A. K. Jha, G. S. Agarwal and R. W. Boyd, Phys. Rev. A **84**, 063847 (2011).
  - [19] G. S. Agarwal, Quantum optics (Cambridge University Press, 2013), p 146.
  - [20] S. Prabhakar et al. Phys. Rev. A **92**, 023822 (2015).
  - [21] A. Einstein, D. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935); E. Schrodinger, Proc. Cambridge Philos. Soc. **31**, 553 (1935); **32**, 446 (1936).
  - [22] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007); S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A **76**, 052116 (2007).
  - [23] A. J. Leggett and A. Garg, Phys. Rev. Lett. **54**, 857 (1985).
  - [24] Y.-N. Chen, C.-M. Li, N.I Lambert, S.-L. Chen, Y. Ota, G.-Y. Chen, and F. Nori, Phys. Rev. A **89**, 032112 (2014); C.-M. Li, Y.-N. Chen, N. Lambert, C.-Y. Chiu, and F. Nori, Phys. Rev. A **92**, 062310 (2015).
  - [25] S.-L. Chen et al., Phys. Rev. Lett. **116**, 020503 (2016).
  - [26] T. Pramanik, M. Kaplan, and A. S. Majumdar, Phys. Rev. A **90**, 050305(R) (2014).
  - [27] J. Oppenheim and S. Wehner, Science **330**, 1072 (2010).
  - [28] P. Chowdhury, T. Pramanik, and A. S. Majumdar, Phys. Rev. A **92**, 042317 (2015).
  - [29] W. Heisenberg, Z. Phys. **43**, 172 (1927).
  - [30] H. P. Robertson, Phys. Rev. **34**, 163 (1929); E. Schrodinger, Sitzungsber. Preuss. Akad. Wiss., Phys. Math. Kl. **19**, 296 (1930).
  - [31] S. Wehner, A. Winter, New J. Phys. **12**, 025009 (2010).
  - [32] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, arXiv:1511.04857.
  - [33] I. Bialynicki-Birula and J. Mycielski, Commun. Math. Phys. **44**, 129 (1975).
  - [34] M. D. Reid, Phys. Rev. A **40**, 913 (1989); S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. **106**, 130402 (2011).
  - [35] P. Chowdhury, T. Pramanik, A. S. Majumdar, and G. S. Agarwal, Phys. Rev. A **89**, 012104 (2014).
  - [36] T. Pramanik, P. Chowdhury, and A. S. Majumdar, Phys. Rev. Lett. **110**, 020402 (2013).
  - [37] T. Pramanik and A. S. Majumdar, Phys. Rev. A **85**,

- 024103 (2012); A. Dey, T. Pramanik, and A. S. Majumdar, Phys. Rev. A **87**, 012120 (2013).
- [38] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. **6**, 845 (2010).
- [39] V. Scarani, S. Iblisdir, N. Gisin, and A. Acn, Rev. Mod. Phys. **77**, 1225 (2005).
- [40] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, Phys. Rev. Lett. **86** 4938 (2001); M. Alexanian, Phys. Rev. A **73**, 045801 (2006) .
- [41] I. Csiszàr and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
- [42] F. Groshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002); C. Weedbrook et al., Phys. Rev. Lett. **93**, 170504 (2004).
- [43] M. F. Pusey, J. Barrett, T. Rudolph, Nature Physics **8**, 475 (2012).
- [44] Note that though we have earlier discussed the analogy between quantum and classical wave mechanics in the context of two-dimensional paraxial optics, for our present purpose correlations among two modes as in the case of classical entanglement and Bell-violation [17] are not required here. At a formal level, the two-dimensional position space wave function may, for example, be taken to be a product of two Gaussians with the uncertainty relations (2), (3) and (4) in classical theory obeyed independently by the two corresponding uncoupled modes. It thus suffices to consider a single mode system for the rest of the analysis presented in this work.